National Phase of PCT/EP99/06312 in U.S.A.

Title: Device for supplying output data in reaction to input data and method for checking authenticity and method for encrypted data transmission

Applicants: OELMAIER; BRAND; HEUER; GERHAEUSER; PROSCH; KORTE; PLANKENBÜHLER

Annotated copy of Final version of PCT/EP99/06312

DEVICE FOR SUPPLYING OUTPUT DATA IN REACTION TO INPUT DATA AND METHOD FOR CHECKING AUTHENTICITY AND METHOD FOR ENCRYPTED DATA TRANSMISSION

[Description]

Field of the Invention

The present invention refers to authenticity checking in manipulation-proof systems and especially to a device for supplying output data in reaction to input data so as to determine the authenticity of the device in dependence upon the output data, and to methods which use such devices.

Background of the Invention and Prior Art

Nowadays integrated circuits are often used, which are applied to a chip card or incorporated in a chip card so as to check whether the owner of the integrated circuits is authorized to carry out a certain action, the authenticity of the integrated circuits being additionally checked so as to provide protection against counterfeited cards. Such integrated circuits are used in the form of smart cards, as defined in the ISO 7816 standard, or in the form of PC cards, as defined in the PCMCIA's PC CARD standard, edition 6.1. Other fields of application, in addition to the above-mentioned possibilities, exist wherever chip cards are used, e.g. in the form of telephone cards or cards permitting access to certain buildings, i.e. cards which serve as electronic keys.

The essential characteristic of the integrated circuits incorporated in such cards is that only the user who is in possession of such a card is actually granted access or is e.g. able to decrypt an encrypted television programme by means of his smart card. The authorization is granted e.g. on the basis of payment, thinking of telephone cards or smart cards in connection with pay TV, or by permitting a specific function, if electronic keys are used.

In order to guarantee that only authorized persons, i.e. persons who acquired e.g. a telephone card, will telephone, it is of decisive importance to identify counterfeited cards and, thinking e.g. of telephone cards, to forbid owners of counterfeited cards to telephone. Al-

though a hundred percent protection against imitators does not exist, it is still possible to present counterfeiters of cards, who simulate the function of the card, with as many difficulties as possible.

Counterfeiters have exhibited great wealth of imagination in copying the functionality of a chip card and of an integrated circuit, respectively. One possibility is e.g. to abrade the chip of a chip card and to infer the functionality of the algorithm implemented on the card from the layout of the integrated circuit. The functionality of the card, i.e. the algorithm which generates on the basis of an input value in the card an output value that is evaluated by a card reader, can then be simulated by means of a computer. When a counterfeiter has ascertained the layout of e.g. a telephone card, he could insert a simulation card, which is connected to a computer, into the card reading slot of a card telephone and simulate the behaviour of the card during the authenticity check.

It goes without saying that there are also mechanical protection mechanisms against such attacks, these protection mechanisms preventing e.g. access from outside to the card when the card has been inserted into a read unit. However, as has been described in the technical publication "Tamper Resistance A Cautionary Note; Proceedings – The Second USENIX Workshop on Electronic Commerce" by Markus Kuhn and Ross Anderson, there are a great number of counterfeiting methods which underline the unabating demand for better protection mechanisms for circuits and especially for integrated circuits on a chip card also in the future. Although conventional data encryption methods, which are based e.g. on the DES algorithm (DES Data Encryption Standard) or which comprise check sum algorithms, provide a high degree of safety when the encryption key, which together with the cryptoalgorithm permits decryption, is kept secret, it is, in principle, also here possible to imitate such an algorithm, which is integrated in a chip card in the form of an integrated circuit in terms of hardware, on the basis of the hardware implementation, i.e. to simulate the functionality of this algorithm e.g. by means of a computer.

Summary of the Invention

It is the object of the present invention to provide a concept for improved protection of electronic circuits and to provide thus a counterfeit-proof check of the authenticity of such electronic circuits and a counterfeit-proof authorization of an owner of such electronic circuits.

[This object is achieved by a device according to claim 1 and by a method according to claim 17 or 18.]

In accordance with a first aspect of the present invention this object is achieved by a device for supplying output data in reaction to input data, said device comprising: an electronic circuit for executing an algorithm that generates the output data on the basis of the input data; and a unit for detecting operational data of the electronic circuit which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, the operational data depending on the input data, said operational data detection unit being coupled to the electronic circuit in such a way that the operational data of the electronic circuit are used by the algorithm, which is executed by said electronic circuit, for generating the output data.

In accordance with a second aspect of the present invention this object is achieved by a method for checking the authenticity of a device to be tested in comparison with an examination device, the device to be tested and the examination device each comprising an electronic circuit for executing an algorithm, which generates output data on the basis of input data, and a unit for detecting operational data which are influenced by an operation of the electronic circuit and which depend on the input data, the operational data detection unit of the device to be tested as well as of the examination device being coupled to the electronic circuit in such a way that the operational data of the electronic circuit are used by the algorithm for producing the output data, said method comprising the following steps: selecting input data; feeding said input data into the device to be tested; in the device to be tested, executing the algorithm by the electronic circuit of the device to be tested, so as to generate the output data on the basis of the input data, detecting operational data of the electronic circuit, which are influenced by an operation of said electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by said electronic circuit, so as to generate the output data; feeding the input data into the examination device; in the examination device executing the algorithm by the electronic

circuit of the examination device so as to generate the output data on the basis of the input data, detecting operational data of the electronic circuit, which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by said electronic circuit, so as to generate the output data; comparing the output data of the device to be tested with the output data of the examination device; and affirming the authenticity of the device to be tested in comparison with the examination device if the output data correspond to one another, in such a way that authenticity will only be affirmed if the operational data of the device to be tested and of the examination device correspond to one another.

In accordance with a third aspect of the present invention this object is achieved by a method for encrypted transmission of information from a first to a second location, the second location being remote from the first location, comprising: producing a random word; feeding the random word into a first device the first device comprising an electronic circuit for executing an algorithm that generates the output data on the basis of the input data; and a unit for detecting operational data of the electronic circuit which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, the operational data depending on the input data, said operational data detection unit being coupled to the electronic circuit in such a way that the operational data of the electronic circuit are used by the algorithm, which is executed by said electronic circuit, for generating the output data, the first device being arranged at a first location; generating the output data of the first device, which depend on the operational data of said first device, by executing an algorithm by the electronic circuit of said first device so as to generate the output data on the basis of the input data, operational data of the electronic circuit being detected, which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by the electronic circuit, so as to generate the output data; encrypting the information with the generated output data as a key; transmitting the encrypted information and the random word from said first location to said second location; feeding the random word into a second device, the second device comprising an electronic circuit for executing an algorithm that generates the output data on the basis of the input data; and a unit for detecting operational data of the electronic circuit which are influenced by an operation of the electronic circuit

when said electronic circuit executes the algorithm, the operational data depending on the input data, said operational data detection unit being coupled to the electronic circuit in such a way that the operational data of the electronic circuit are used by the algorithm, which is executed by said electronic circuit, for generating the output data, the second device being positioned at the second location; generating the output data of the second device, which depend on the operational data of said second device, by executing the algorithm by the electronic circuit of said second device, so as to generate the output data on the basis of the input data, operational data of the electronic circuit being detected, which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by the electronic circuit, so as to generate the output data; decrypting the encrypted information making use of the output data of the second device as a key, the decrypted information corresponding to the original information prior to encrypting if the operational data of the first device at the first location correspond to the operational data of the second device at the second location.

The present invention is based on the finding that it is comparatively simple to imitate the functionality of a chip, but that it is much more difficult to imitate its time or power behaviour. A device for supplying output data in reaction to input data so as to determine the authenticity of the device in dependence upon said output data comprises therefore, on the one hand, an electronic circuit for executing an algorithm that generates the output data on the basis of the input data, and, on the other hand, a unit for detecting operational data which are influenced by an operation of the electronic circuit, the data detection unit being coupled to the electronic circuit in such a way that the operational data of the electronic circuit are used by the algorithm for generating the output data.

According to a preferred embodiment of the present invention, the electronic circuit implements an cryptographic algorithm which calls the operational data detection unit so as to carry out time and/or power measurements which, in addition to the input data, are used by the electronic circuit so as to generate the output data. Hence, the output data represent a combination of the functionality of the cryptographic algorithm and of the operational data of the circuit used for executing the cryptographic algorithm. An attack on the device according to the present invention must therefore simulate not only the cryptographic algorithm but

also the power consumption and/or the time behaviour of the electronic circuit during the execution of the cryptographic algorithm.

A large number of cryptographic algorithms is shown in the technical book "Applied Cryptography" by Bruce Schneier.

Operational data of the integrated circuit which are used for generating the output data are preferably the power consumption and the run time of the algorithm in the electronic circuit. Such operational or "environmental" data may, however, be all the data which are influenced by an operation of the electronic circuit, such as an electromagnetic radiation emitted by the electronic circuit and the like. Limits to the use of operational data are the possibilities of measuring these operational data in a practical implementation, thinking e.g. of electromagnetic radiation. Hence, the data which are preferably used as operational data because they are easy to measure are power data and data concerning the time behaviour of the electronic circuit.

In principle, it will not be necessary that the algorithm is a cryptographic algorithm. It might be any algorithm which has different operational data in dependence upon different input data. However, the protection against counterfeiting will be the better the "more chaotic" the dependence of the operational data on different input data is.

In order to improve protection, the algorithm used is preferably a cryptoalgorithm which provides protection against counterfeits per se, this protection being enhanced by the fact that, according to the present invention, the operational data of the electronic circuit executing this cryptographic algorithm are taken into account. Normally, algorithms are, however, designed such that they have a comparatively constant run time behaviour independently of the input values. In order to improve the safety still further, the algorithm executed by the electronic circuit will preferably comprise two sub-algorithms, i.e. one cryptographic algorithm and one test algorithm which is programmed exclusively in such a way that its operating behaviour will be as "chaotic" as possible in dependence upon different input data.

In the calculation of the output data, which are used for checking the authenticity of the device, the results of the test algorithm are, however, not taken into account, but the data taken into account are only the operational data of the electronic circuit which executes the

test algorithm and the output data of the cryptoalgorithm; hence, a counterfeiter will find it even more difficult to attack the test algorithm, since, in the most advantageous case, he will only find out the input data into the test algorithm but no output data.

The safety will be enhanced still further in particular by the use of a multi-step cryptoalgorithm and by the additional use of a multi-step test algorithm; for one step of the cryptoalgorithm also the operational data of the test algorithm, which have been generated by the execution of the preceding step of the test algorithm, are used in addition to the intermediate result of the preceding step of the cryptoalgorithm. This "interleaving" of a multi-step cryptoalgorithm with a multi-step test algorithm provides a high degree of safety against counterfeits.

In contrast to former attempts to counterfeit, which tried to identify the structure of a chip making use of different methods and which then used these data so as to analyze the functionality of a chip and integrate it into another chip, or simulate it by a computer, counterfeiters who attack the device according to the present invention must redesign the chip completely and perhaps they must even expressly direct the production method thereto. This is necessary because it is not only the functionality of the chip that has to be simulated but also the operating behaviour of the electronic circuit, i.e. the hardware. In contrast to the prior art, where attempts were made to achieve safety by means of increasingly elaborate functionalities, the present invention aims at incorporating hardware aspects into the safety in such a way that a counterfeiter may even have to use exactly the same process for producing integrated circuits so as to simulate identical power and run time data for simulating, i.e. counterfeiting, an authentic device.

Brief Description of the Drawings

In the following, preferred embodiments of the present invention will be explained in more detail making reference to the drawings enclosed, in which:

Fig. 1 shows a schematic representation of a device according to the present invention;

Fig. 2 shows a preferred embodiment according to the present invention;

Fig. 3 shows how a cryptoalgorithm and a test algorithm co-operate according to a preferred embodiment of the present invention;

Fig. 4 shows a flow chart for a method for checking the authenticity making use of two devices according to the present invention; and

Fig. 5 shows a flow chart of a method for encrypted transmission of information from a first location to a second location making use of two devices according to the present invention.

Detailed Description of Preferred Embodiments

Fig. 1 shows as a schematic circuit diagram a device 10 according to the present invention for supplying output data 12 in reaction to input data 14 so as to determine the authenticity of the device 10 in dependence upon the output data 12. The device 10 comprises an electronic circuit 16 for executing an algorithm that generates the output data 12 on the basis of the input data 14, and a unit 18 for detecting operational data that are influenced by an operation of the electronic circuit 16, the operational data detection unit 18 being coupled to the electronic circuit 16 in such a way that the operational data of the electronic circuit 16 are used by the algorithm in order to generate the output data 12.

The operational data detection unit 18 detects preferably an elapsed calculation time or the power consumption of the electronic circuit 16 for executing an algorithm. In contrast to the functionality executed by the algorithm, which is implemented by the electronic circuit 16, the operational data are also referred to as environmental data. Such environmental data may be all data which are suitable for describing the operation of a chip, i.e. of an electronic circuit, e.g. the electromagnetic radiation emitted by the electronic circuit 16. A limit only exists with respect to the technical possibilities of integrating measurement means in the device 10.

The device 10 is preferably produced in an integrated form and implemented as smart card, PC card, telephone card, electronic key and the like. The measurement of the operational

data by the unit 18 is then carried out on the card itself. Hence, time data and power data are preferred as operational data, since they can be measured easily.

The measurement of the instantaneous power consumption can be realized by a comparatively simple electronic network comprising a resistor, a capacitor and an analog-digital converter. This circuit arrangement should be as precise as possible. Due to variations of the input power and of the properties of the materials used, the accuracy is, however, a limited one, since repeated executions with the same input values must produce precisely the same results independently of the environmental conditions.

Fig. 2 shows a slightly more detailed view of the device 10 according to the present invention in accordance with a preferred embodiment of the present invention. The electronic circuit 16 for executing an algorithm is subdivided into two sub-circuits 16a and 16b, sub-circuit 16a being capable of executing a cryptoalgorithm, whereas sub-circuit 16b is capable of executing a test algorithm.

The operational data detection unit 18 is also bipartite and comprises time measuring means 18a and, in addition, power measuring means 18b.

The time measurement by means of the operational data detection unit 18 should be carried out by means of an internal clock chip, since a supplied clock might vary excessively. Time control should be as precise as possible, since repeated executions must produce the same results. Time measurements can be carried out on the basis of the clock of the chip; this will, however, necessitate safety-relevant compromises, since it is then not the actual speed of the electronic circuit 16 that is relevant, but only the clock cycles per command are decisive.

Due to the fact that operational data of the device 16 are used, the algorithm executed by the device 16 is made hardware dependent. Simultaneously, these measurement values must, however, be reproducible in a reliable manner in such a way that, when the authenticity is checked, incorrect results caused by parameter variations will be avoided. On the other hand, the demands on the operational data, i.e. the manufacturing tolerances for producing a device to be tested and a testing device, should be chosen as narrow as possible so as to achieve a high degree of safety.

With respect to time measurement the means 18a is preferably arranged so as to measure absolute times with the aid of an independent clock chip integrated in the means 18a. A higher degree of safety is achieved in this way, but also a dependence on external clock generators whereby the portability from one equipment to the next will deteriorate.

In the case of the power measurement means 18b the hardware dependence entails certain problems. Digitizing errors of the analog-digital converter, which is contained in the power measurement means 18b, may render the results unpredictable. This problem can either be solved by using very high sampling rates and by rounding generously or it can be solved by implementing complicated noise-reduction algorithms in the power measurement means 18b. Another possibility of trying to solve this problem is the use of pattern recognition algorithms which provide certain classification numbers on the basis of the recorded signals, i.e. time or power consumption values, which can be used by this pattern recognition algorithm. In this case the device 10 is hardware-dependent insofar as the data used are not absolute operational data but that specific "characteristics", i.e. the power consumption as a function of time, or certain calculation times of individual algorithm steps are used so as to achieve the additional safety aspect of hardware dependence.

With respect to the architecture of the combination of the algorithm executed by the electronic circuit 16 and with respect to the operational data two possibilities are mentioned, only by way of example. One possibility is referred to as test point architecture. An external control coupled to the device 16 e.g. via an auxiliary input interrupts the execution of the algorithm by the electronic circuit 16 e.g. after a certain number of clock cycles or seconds. Subsequently, a "snapshot" of the execution state of the electronic circuit 16 is taken. This snapshot comprises e.g. data with respect to the progress of the algorithm, register states, the power that has been consumed since the last test point or the time that has been consumed since the last test point. This architecture does not necessitate a division of the algorithm into parts. If, however, clock cycles are not used for measuring the time, this possibility is difficult to implement in reality, since a slower execution of the algorithm in view of external conditions may change a snapshot completely. In addition, a snapshot cannot be rounded, as has already been mentioned. In most cases, the amount of data collected is, moreover, too large; hence data have to be combined. A combinatorial algorithm depends

on the data recorded during the snapshot and may range from a simple XOR operation to complex check sum algorithms, such as "Message-Digest algorithms".

The second possibility, which is referred to as "demand architecture", is therefore preferred. This possibility is schematically shown in Fig. 3. Fig. 3 shows the interleaving of a cryptoalgorithm 16a with a test algorithm 16b. The cryptoalgorithm 16a, which may e.g. be a DES algorithm that is subdivided into n steps, receives in step 1 the input data 14. In addition, also a test algorithm 16b, which will be discussed in detail hereinbelow, is composed of n steps and also this test algorithm receives the input data 14 in its step 1.

When the cryptoalgorithm 16a has calculated the first step, it provides a certain intermediate result. The first step of the test algorithm 16b does not provide the results of the test algorithm, which are not of interest, but it supplies the operational data thereof as input signal to the second step of the cryptoalgorithm 16a, as shown by an arrow 20. This process is repeated for each of the n steps in such a way that each step of the cryptoalgorithm 16a receives as an input signal the intermediate result of the last step of the cryptoalgorithm as well as the operational data of the test algorithm of the last step. This architecture is called demand architecture, since either the cryptoalgorithm itself or a control demands from the test algorithm the execution of measurements of operational data and the subsequent transmission of the operational data to the cryptoalgorithm.

Although it has been said up to now that, if the cryptoalgorithm as well as the test algorithm are executed by the electronic circuit 16, the results of the test algorithm will not be taken into account and that only the operational data of the electronic circuit, which executes the test algorithm, will in this case be taken into account in the production of the output data 12, it is, of course, also possible to include the result data of the test algorithm in the cryptoalgorithm. Due to the fact that the result data of the test algorithm are, however, rejected in the device itself and do not appear externally at all, a counterfeiter will find it much more difficult to draw conclusions with respect to the test algorithm for simulating the operational behaviour of this test algorithm so as to obtain the operational data, since in the most favourable case for him he will only know the input data 14 inputted in this test algorithm and the operational data, but not the output data. Hence, it will be almost impossible for him to simulate the functionality of the test algorithm so as to be able to draw conclusion with respect to the operational data.

In principle, it would also be possible to simulate the operational data with some other algorithm having similar operational conditions. If, however, a test algorithm of sufficient complexity is used, e.g. an algorithm for calculating fractals, it is indeed almost impossible to simulate the operational behaviour of the test algorithm without knowing the result data. Even if the functionality of the test algorithm should be obtained, with very great effort, from the layout of the integrated circuit executing this test algorithm, the safety aspect of the present invention is to be see in that the functionality as such is of no use at all, but that in addition to the functionality also the operational behaviour of the electronic circuit 16 would have to be simulated. Furthermore, a counterfeiter will a priori not know whether or not the operational data of the test algorithm are fed into the cryptoalgorithm, nor will he know which combinations or correlations thereof exist. It goes without saying that it would be possible to take the result data of the test algorithm into account only in the case of a few steps and to include, in the case of the other steps, only the operational data into the execution of the cryptoalgorithm.

It follows that, for the present invention, it is not absolutely necessary to measure the operational behaviour of the cryptographic algorithm or cryptoalgorithm. As can be seen from Fig. 3 and has already been described to a sufficient extent, a test algorithm can be executed by the electronic circuit 16, this test algorithm being preferably a complex and difficult algorithm whose behaviour is hard to predict or "pseudo-chaotic". When, in the simplest case, input signals of different lengths produce different operational data and when the algorithm as such is kept secret, a good protection has already been achieved, since a counterfeiter who wants to simulate the functionality of the algorithm will not be able to produce an authentic card, since the output data are not the result data of the test algorithm, but, in the simplest case, the operational data. In order to improve the version employing the test algorithm alone, it will, of course, be possible to use not only the operational data alone for the production of the output data, but the result data may also be combined with the operational data in some way or other. The best protection will, however, be achieved, when the test algorithm is combined with the cryptoalgorithm, e.g. in the manner shown in Fig. 3.

The test algorithm should use special features of the electronic circuit 16, whereby attacks will be made even more difficult. Furthermore, this algorithm should not exhibit a simple run time behaviour, which might be of such a nature that higher-order input signals result in

slower calculations. Such a behaviour would again have the effect that the operational behaviour of the electronic circuit 16, which executes the algorithm, would be made predictable in a way. Hence, the input signal can be randomized e.g. by means of a series of XOR operations or it can sent through a function with "pseudo-chaotic" behaviour in such a way that, although there is a defined relationship between the output signal of the function and the input signal, this relationship is extremely complicated and a functional relationship cannot be seen merely by viewing. In this case, the test algorithm itself comprises two parts, viz. a first part which renders the input signal random or at least highly unpredictable and a second part which is the actual test algorithm so as to be able to determine the timing or the power consumption of the integrated circuit 16.

Fig. 4 shows a flow chart for a method of checking the authenticity of a device; this kind of method could be executed e.g. by an electronic door lock, so that only the owner of an authentic "key card" is allowed to pass the door. Such an electronic door lock normally comprises a microcontrol and a card-read/write unit into which a card provided with the device according to the present invention can be inserted as well as a fixedly installed card-read/write unit in which a reference card, which is provided with the device according to the present invention as well, is fixedly installed and arranged such that it is not accessible from outside. The reference or examination device corresponds to the device to be tested insofar as these devices both originate e.g. from the same product batch so that their hardware will be identical so as to exhibit the greatest possible likelihood in their operational behaviour.

When the owner of a card wants to pass through a door which is provided with an electronic key system of this type, he will insert his card, which has attached thereto the device according to the present invention, in the card reader.

The method of checking the authenticity of the inserted device, i.e. of the device to be tested, is shown in Fig. 4. The microcontrol first selects arbitrary random input data (block 40). In a next step, these input data are fed into the device to be tested as well as into the examination device (block 42). The device to be checked by the user with respect to its authenticity, i.e. the device to be tested, as well as the examination device, which is preferably fixedly installed in the door lock, now execute parallel to one another the same steps and produce output data, the output data of the examination device depending on the operational data of the electronic circuit 16 of the examination device and the output data of the

device to be tested depending on the operational data of the electronic circuit 16 of the device to be tested.

The output data of the two devices are compared in a block 44. If these output data correspond, the authenticity of the device to be tested will be affirmed (block 46). If the output data do not correspond, the authenticity of the device to be tested will be denied (block 48) and the door lock will not be opened. In this case, both the device to be tested and the examination device are "operated" by one and the same microcontrol. This means that e.g. an external clock for measuring the time behaviour, which is coupled with the operational data detection unit 18, will be identical for both devices. In this case, the operational data can be detected with extremely high accuracy, since clock fluctuations or the like will affect the two devices alike and will therefore not lead to a divergence between the two devices.

This method which consists in that a device has supplied thereto an input signal in such a way that it produces an output signal, the output signal being judged in dependence upon the input signal, is also referred to as "challenge-response" algorithm. Preferably, some random input signal is supplied to the device which then calculates a result by means of the electronic circuit 16 and outputs the collected operational data, i.e. processes them in the output data. The verification takes place on the basis of a comparison with a reference or examination device. For an attacker it would, in principle, be possible to listen in to the data communication between the device to be tested and the microcontrol within the card reader, which has to be accessible from outside per definition. Since, in the case of the preferred embodiment of the present invention shown in Fig. 3, the operational data are, however, only processed within the device according to the present invention and are not transmitted to the outside world and since, in addition, also the result data of the test algorithm remain within the device and are not transmitted to the outside world and are not even taken into account at all, listening in to the data communication will not be a great help to a person attacking the device according to the present invention. Hence, the device according to the present invention comprises three secrecy aspects, viz. firstly a conventional secret password for the cryptoalgorithm, secondly the secret test algorithm and finally the concrete hardware design of the electronic circuit 16.

The concept of feeding operational data into respective subsequent steps of a cryptoalgorithm, which is the DES algorithm in the preferred embodiment, leads to the preferred use of

one-way street functions for safety reasons. This means that on the basis of certain input data only output data can be calculated, but that functionally calculating back from these output data to the input data is impossible, since the use of the operational data determines a chronological sequence of calculation. When the authenticity of a device to be tested is checked in the way shown in Fig. 4, an inversion of the functionality is not even necessary, since both the device to be tested and the examination device execute a one-way-street function in parallel and need not use an inverted calculation sequence under any circumstances.

Safety can be increased still further, when special processors are used for the electronic circuit 16, which are optimized for specific operations in such a way that a standard chip or a computer will not be able to simulate the time response of certain processors.

A further improvement is to be seen in the circumstance that the test algorithm, whose results are not used in the preferred embodiment shown in Fig. 3 and which is only provided for generating the operational data, can be exchanged every now and then. Such an exchange of the test algorithm can be carried out in a flexible manner; attention should only be paid to the fact that the device to be tested and the examination device have the same test algorithm so as to have identical operational data in the case of an authentic card.

The present invention can be applied to almost any cryptographic algorithm, i.e. cryptoalgorithm. An additional advantage of the present invention is to be seen in the fact that the present invention can be integrated in existing safety systems.

Fig. 5 shows a further possibility of using the device according to the present invention taking as an example the encrypted transmission of information from one location to another location, this kind of transmission taking place e.g. in the case of "pay TV". The information to be encrypted must first be encrypted in a transmitter. For this purpose, the transmitter includes a smart card which is provided with a device according to the present invention. The transmitter first selects random input data as password character chain (block 50). In a block 52, the input data 14 are fed into the transmitter smart card which generates output data 12 in a step 54. The information to be encrypted is now encrypted making use of the output data 12, which have been generated by the transmitter smart card, as a key (block 56). The encrypted information together with the output data selected in block 50 are now

transmitted from one location to the other location, i.e. from the transmitter to the receiver, (block 58).

Reference should be made to the fact that, on the one hand, the information is now encrypted and can therefore only be decrypted by a person who acquired a suitable authorization, e.g. in the form of a receiver smart card. On the other hand, the key for encrypting the information is not explicitly transmitted, but what is transmitted are only the input data in the transmitter smart card. A user who does not possess an authorized receiver smart card having the same operational data as the transmitter smart card will not be able to generate on the basis of the input data 14 the correct output data 12 which are required for decrypting the encrypted information.

The first operation to be executed in the receiver is to extract the input data from the transmission, which comprises the encrypted information as well as the input data, (block 60). The input data extracted in block 60 are now fed into the receiver smart card (block 62), which, provided that it is an authentic receiver smart card, will have the same operating behaviour as the transmitter smart card and will therefore produce the same output data from the input data (block 64). Finally, the encrypted information is decrypted in a block 66 making use of the output data of the receiver smart card.

If the receiver smart card is a counterfeited card, which does not have the same operating behaviour as the transmitter smart card, this will not be recognized immediately in the case of the method shown in Fig. 5, since, unlike Fig. 4, an authenticity check is not carried out. The output data, which are required as a key for decrypting, will, however, not correspond to the output data which have been used in block 54 for encrypting, and, consequently, correct decrypting of the encrypted information will not be possible. This means that, in the most simple case, a counterfeited smart card will not be objected to in the receiver immediately, but that, although it will provide output data 12 on the basis of operational data that differ from those of the transmitter smart card, a correct decryption will, however, not be possible on the basis of the output data provided; hence, a counterfeited card will be of no use to the counterfeiter.

It follows that the present invention comprises an electronic circuit, which is preferably integrated, and a means for supervising the operation of the electronic circuit by measuring

data, the operation of the electronic circuit including the execution of an algorithm which provides output data as the result of a preferably complex calculation. These output data are, however, influenced, by the measured operational data. Preferably, the measured data comprise time or power consumption data. The device according to the present invention can arbitrarily be accommodated on cards, e.g. smart cards or PC cards, electronic keys and the like.

CLAIMS

1. A device [(10)] for supplying output data [(12)] in reaction to input data [(14)] [so as to determine the authenticity of the device (10) in dependence upon said output data (12)], said device [(10)] comprising:

an electronic circuit [(16)] for executing an algorithm that generates the output data [(12)] on the basis of the input data [(14)]; and

a unit [(18)] for detecting operational data of the electronic circuit which are influenced by an operation of the electronic circuit [(16)] when said electronic circuit executes the algorithm, the operational data depending on the input data,

said operational data detection unit [(18)] being coupled to the electronic circuit [(16)] in such a way that the operational data of the electronic circuit are used by the algorithm, which is executed by said electronic circuit [(16)], for generating the output data [(12)].

2. A device [(10)] according to claim 1, wherein the operational data are selected from the group comprising time data and power data.

3. A device [(10)] according to claim 1 [or 2], wherein the electronic circuit [(16)] and the detection unit [(18)] are integrated as a unit.

4. A device [(10)] according to [one of the preceding claims] claim 1, which is contained in a smart card or in a PC card.

5. A device [(10)] according to [one of the preceding claims] claim 1, wherein the electronic circuit [(16)] is arranged so as to execute an cryptoalgorithm.

6. A device [(10)] according to [one of the claims] claim 1 [to 4], wherein the electronic circuit [(16)] is arranged so as to execute a check sum algorithm.

7. A device [(10)] according to claim 5, wherein the cryptoalgorithm is a multi-step algorithm, the operational data of one algorithm step being used as input data for the subsequent algorithm step.

8. A device [(10)] according to [one of the claims 1 to 6] claim 1, wherein the electronic circuit [(16)] is arranged so as to stop the operation after a predetermined execution time during execution of the algorithm and wherein the detection unit [(18)] is arranged so as to feed operational data into the algorithm at said predetermined execution time.

9. A device [(10)] according to [one of the claims 1 to 3] claim 1, wherein the algorithm is of such a nature that it will first randomize the input data [(14)], whereby the dependence of the operational data on the input data will be pseudo-random.

10. A device [(10)] according to claim 9, wherein the output data generated by the algorithm are only the operational data.

11. A device [(10)] according to [one of the claims 1 to 4] claim 1, wherein the electronic circuit [(16)] comprises two sub-circuits [(16a, 16b)] which each execute a sub-algorithm, the first sub-algorithm being a test algorithm whose operational data are detected by the detection unit [(18)], and the second sub-algorithm being a cryptoalgorithm or a check sum algorithm, the operational data of the test algorithm being processed in the cryptoalgorithm.

12. A device [(10)] according to claim 11, wherein the second sub-circuit [(16a)] is arranged so as to execute the DES algorithm which comprises n steps, and wherein the first sub-circuit [(16b)] is arranged so as to execute a test algorithm which also comprises n steps, the input data being adapted to be fed into the first step of the DES algorithm as well as into the first step of the test algorithm, and data which are adapted to be fed into a further step of the DES algorithm being result data of the first step of the DES algorithm and operational data of the first step of the test algorithm, whereas a result of one step of the test algorithm is rejected.

13. A device [(10)] according to [one of the preceding claims] claim 1, wherein the operational data detection unit comprises a time measuring means [(18a)] and a power measuring means [(18b)] for measuring the time which the electronic circuit [(16)] needs for execut-

ing a specific task and for measuring the power consumed when said specific task is being executed.

14. A device [(10)] according to claim 13, wherein the power measuring means [(18b)] comprises a resistor, a capacitor and an analog-digital converter for measuring the power consumed.

15. A device [(10)] according to claim 13 [or 14], wherein the time measuring means comprises an internal clock generator.

16. A device [(10)] according to [one of the preceding claims] claim 1, wherein the operational data detection unit [(18)] comprises a pattern recognition algorithm so as to produce the operational data from power or time parameters of the electronic circuit [(16)].

17. A method for checking the authenticity of a device [(10)] to be tested in comparison with an examination device [(10)], the device [(10)] to be tested and the examination device [(10)] each comprising an electronic circuit [(16)] for executing an algorithm, which generates output data [(12)] on the basis of input data [(14)], and a unit [(18)] for detecting operational data which are influenced by an operation of the electronic circuit [(16)] and which depend on the input data, the operational data detection unit [(18)] of the device to be tested as well as of the examination device being coupled to the electronic circuit [(16)] in such a way that the operational data of the electronic circuit are used by the algorithm for producing the output data, said method comprising the following steps:

selecting [(40)] input data;

feeding [(42)] said input data into the device [(10)] to be tested;

in the device to be tested,

executing the algorithm by the electronic circuit of the device to be tested, so as to generate the output data on the basis of the input data,

detecting operational data of the electronic circuit, which are influenced by an operation of said electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by said electronic circuit, so as to generate the output data;

feeding [(42)] the input data into the examination device [(10)];

in the examination device

executing the algorithm by the electronic circuit of the examination device so as to generate the output data on the basis of the input data,

detecting operational data of the electronic circuit, which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by said electronic circuit, so as to generate the output data;

comparing [(44)] the output data of the device to be tested with the output data of the examination device; and

affirming [(46)] the authenticity of the device to be tested in comparison with the examination device if the output data correspond to one another, in such a way that authenticity will only be affirmed if the operational data of the device to be tested and of the examination device correspond to one another.

18. A method for encrypted transmission of information from a first to a second location, the second location being remote from the first location, comprising:

producing [(50)] a random word;

feeding [(52)] the random word into a first device [(10)] [according to one of the claims 1 to 16] the first device comprising an electronic circuit for executing an algorithm that generates

the output data on the basis of the input data; and a unit for detecting operational data of the electronic circuit which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, the operational data depending on the input data, said operational data detection unit being coupled to the electronic circuit in such a way that the operational data of the electronic circuit are used by the algorithm, which is executed by said electronic circuit, for generating the output data, the first device [which is] being arranged at a first location;

generating [(54)] the output data of the first device, which depend on the operational data of said first device, by executing an algorithm by the electronic circuit of said first device so as to generate the output data on the basis of the input data, operational data of the electronic circuit being detected, which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, said operational data depending on the input data, and said detected operational data of the electronic circuit being used by the algorithm, which is executed by the electronic circuit, so as to generate the output data;

encrypting [(56)] the information with the generated output data as a key;

transmitting [(58)] the encrypted information and the random word from said first location to said second location;

feeding [(62)] the random word into a second device [implemented according to one of the claims 1 to 16 and], the second device comprising an electronic circuit for executing an algorithm that generates the output data on the basis of the input data; and a unit for detecting operational data of the electronic circuit which are influenced by an operation of the electronic circuit when said electronic circuit executes the algorithm, the operational data depending on the input data, said operational data detection unit being coupled to the electronic circuit in such a way that the operational data of the electronic circuit are used by the algorithm, which is executed by said electronic circuit, for generating the output data, the second device being positioned at the second location;

generating [(64)] the output data [by means of the second device which is positioned at said second location] of the second device, which depend on the operational data of said second device, by executing the algorithm by the electronic circuit of said second device, so as to

DEVICE FOR SUPPLYING OUTPUT DATA IN REACTION TO INPUT DATA AND METHOD FOR CHECKING AUTHENTICITY AND METHOD FOR ENCRYPTED DATA TRANSMISSION

Abstract

A device [(10)] for supplying output data [(12)] in reaction to input data [(14)], so as to determine the authenticity of the device in dependence upon the output data [(12)], comprises an electronic circuit [(16)] for executing an algorithm, which generates the output data [(12)] on the basis of said input data [(14)], and a unit [(18)] for detecting operational data which are influenced by an operation of the electronic circuit [(16)]. The operational data detection unit [(18)] is coupled to the electronic circuit [(16)] in such a way that the operational data of the electronic circuit [(16)] are used by the algorithm for generating the output data [(12)]. Safety of the device according to the present invention is enhanced in that a potential counterfeiter will have to simulate not only the functionality of the device but also hardware features of the device, such as power consumption or time response, in order to simulate an authentic card.

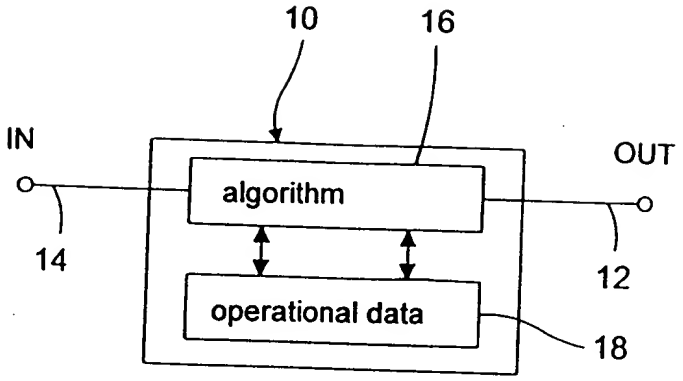
10
16
IN
OUT
algorithm
14
12
operational data
18

FIG.1

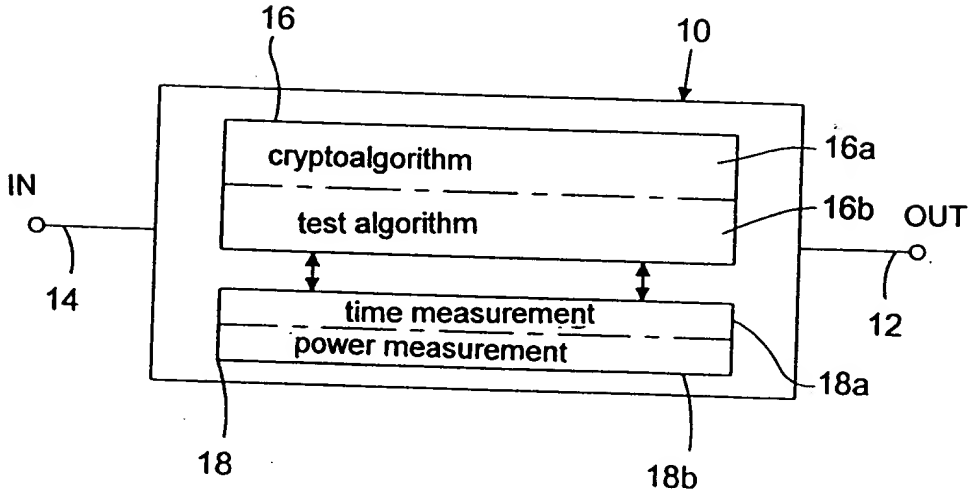
16
10
cryptoalgorithm
16a
IN
test algorithm
16b
OUT
14
time measurement
power measurement
12
18a
18
18b

FIG.2

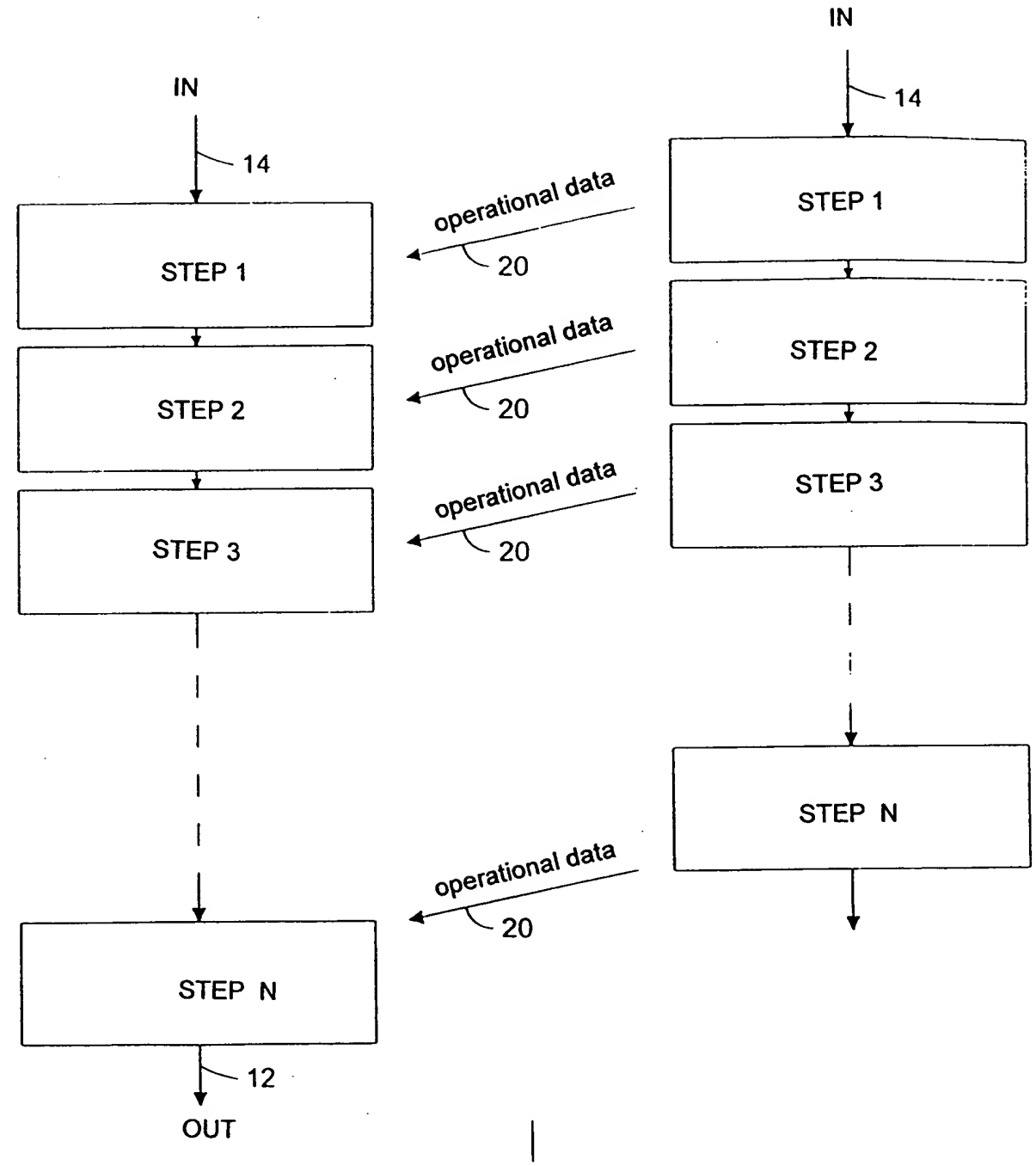
IN
14
STEP 1
STEP 2
STEP 3
STEP N
12
OUT
operational data
20
operational data
20
operational data
20
operational data
20
IN
14
STEP 1
STEP 2
STEP 3
STEP N
cryptoalgorithm (16a)
test algorithm (16b)

FIG.3

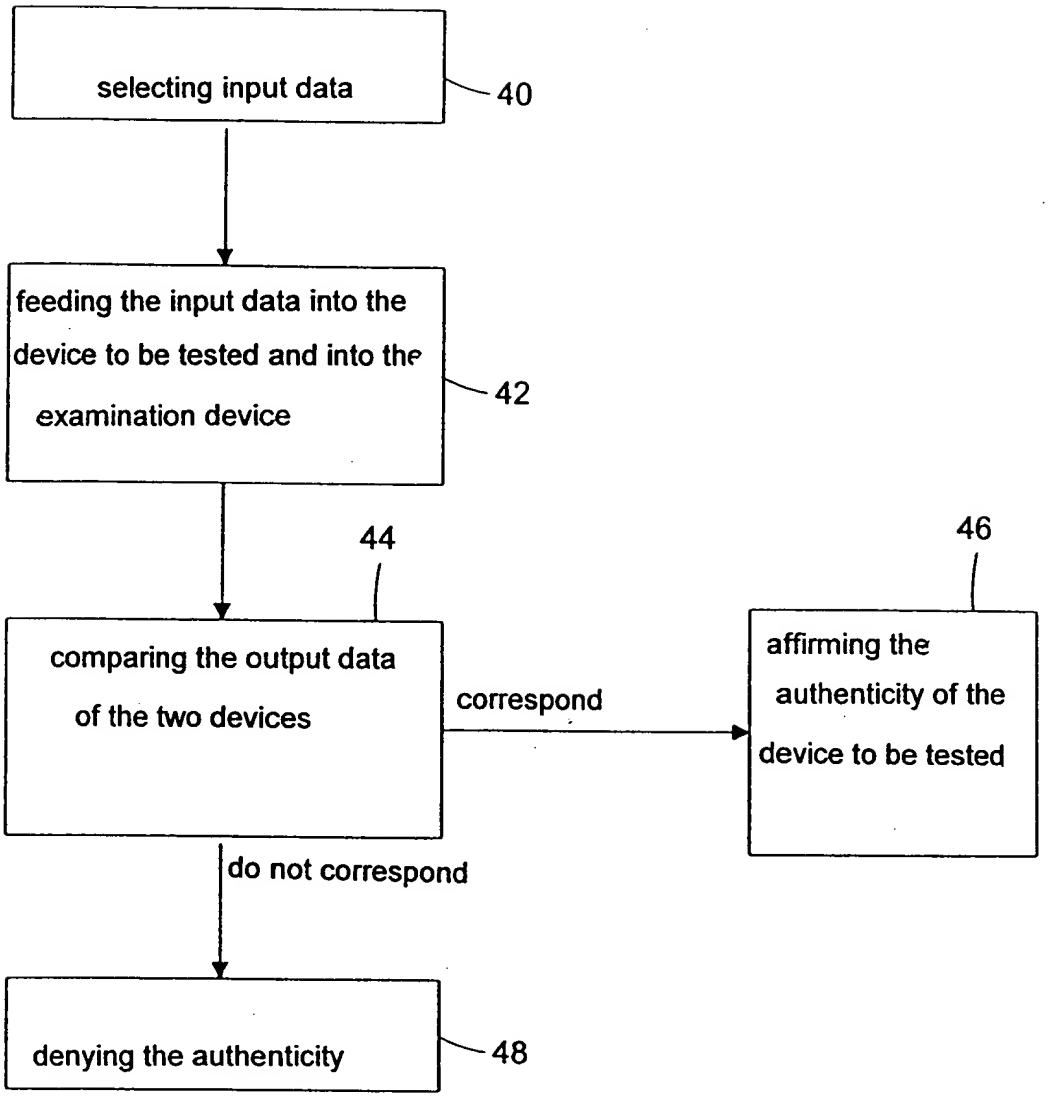
selecting input data
40
feeding the input data into the device to be tested and into the examination device
42
44
comparing the output data of the two devices
correspond
46
affirming the authenticity of the device to be tested
do not correspond
denying the authenticity
48

FIG.4

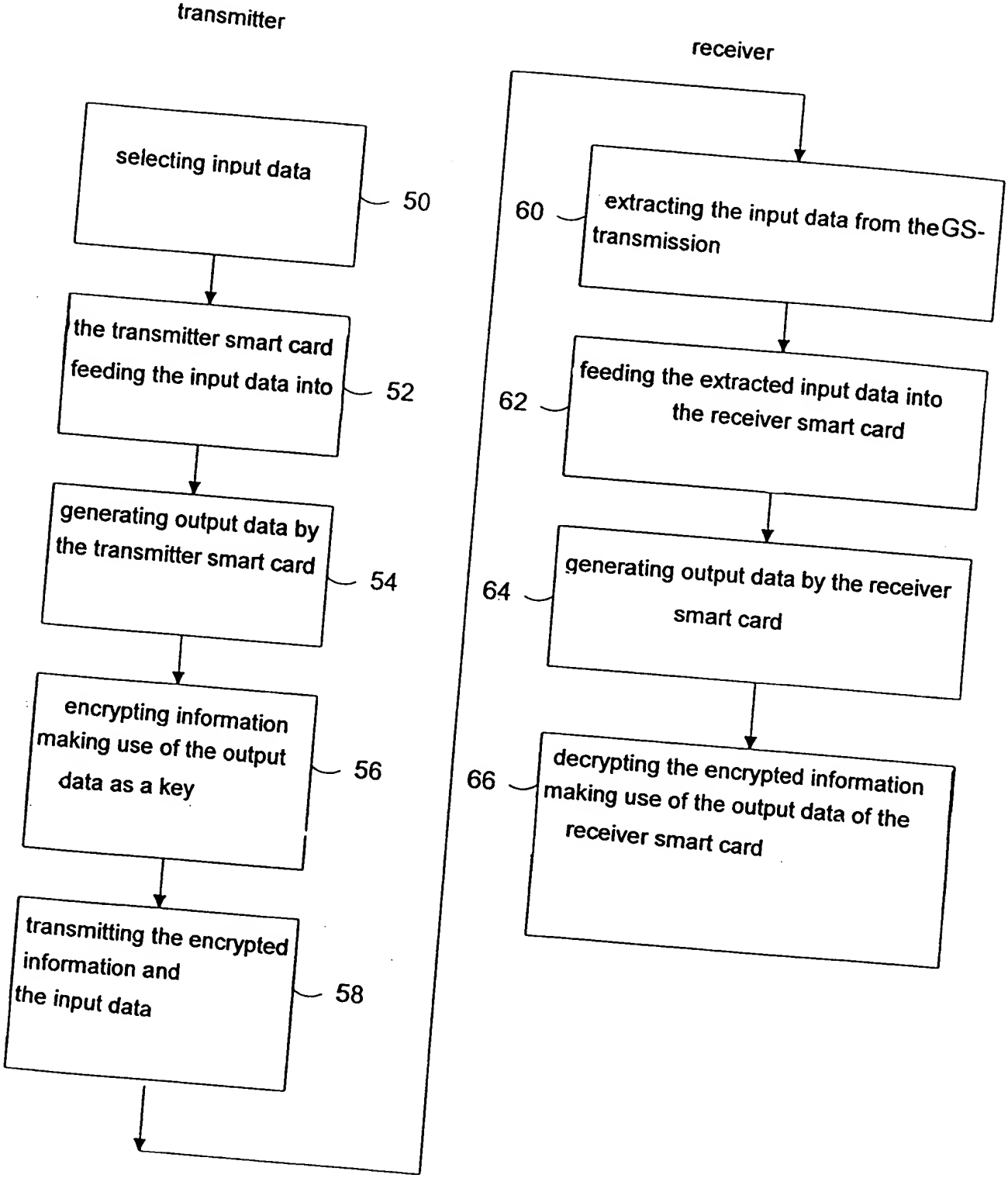
transmitter
receiver
selecting input data
50
the transmitter smart card feeding the input data into
52
generating output data by the transmitter smart card
54
encrypting information making use of the output data as a key
56
transmitting the encrypted information and the input data
58
60
extracting the input data from the GS-transmission
62
feeding the extracted input data into the receiver smart card
64
generating output data by the receiver smart card
66
decrypting the encrypted information making use of the output data of the receiver smart card

FIG.5